WHAT IS CLAIMED IS:

1. A computer-implemented method for generating access control information, the method comprising:

receiving an access control rule that identifies a characteristic;

identifying at least one entry in user information that is associated with the identified characteristic;

identifying at least one entry in data object information that is associated with the identified characteristic; and

generating access control information that permits at least one user associated with the at least one entry in the user information to access the at least one entry in the data object information.

2. The method of claim 1 wherein:

the identified characteristic is indirectly associated with the at least one entry in the user information, and

identifying at least one entry in user information that is associated with the identified characteristic comprises identifying at least one entry in user information that is indirectly associated with the identified characteristic .

3. The method of claim 1 wherein:

the identified characteristic is directly associated with the at least one entry in the user information, and

identifying at least one entry in user information that is associated with the identified characteristic comprises identifying at least one entry in user information that is directly associated with the identified characteristic.

4. The method of claim 1 wherein generating access control information comprises:

generating user access control information that identifies the at least one entry in the user information that is associated with the identified characteristic,

generating object access control information that identifies the at least one entry in the data object information that is associated with the identified characteristic, and

associating at least one entry in the user access control information with at least one entry in the data object access control information.

5. The method of claim 4 further comprising storing the association of the at least one entry in the user access control information with the at least one entry in the data object access control information.

6. The method of claim 4 further comprising:

storing the data object access control information, and

storing the user access control information.

7. The method of claim 4 further comprising determining whether a particular user associated with the at least one entry in the user access control information is permitted access to a particular data object that is associated with the at least one entry in the data object access control information wherein the determination is based on the association of the at least one entry in the user access control information with the at least one entry in the data object access control information.

8. The method of claim 1 further comprising receiving a filter condition, wherein generating access control information further comprises generating access control information by eliminating at least one entry in the user information that corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the user information.

9. The method of claim 1 further comprising receiving a filter condition, wherein generating access control information further comprises generating access control information by eliminating at least one entry in the data object information that corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the data object information.

10. A computer system for managing access control information for software operating on the computer system, the system comprising:

a data repository for access control information for software, the data repository including user information identifying a user characteristic for at least one entry in the user information, data object information identifying a data object characteristic for at least one entry in the data object information, and access control rule information identifying a shared characteristic for at least one entry in the access control rule information; and

an executable software module that causes (1) a comparison of the user characteristic, the business object characteristic, and the shared characteristic and (2) generation of access control information for use in determining whether a user that is associated with an entry in the user information is permitted to access a data object that is associated with an entry in the data object information such that when the user characteristic, the data object characteristic and the shared characteristic each correspond to one another, the user is permitted to access the data object.

11. The computer system of claim 10 further comprising a second executable software module that causes a determination whether a user associated with an entry in the user information is permitted to access a data object associated with an entry in the data object information such that the determination is based on the generated access control information.

12. The computer system of claim 11 wherein the second executable software module is the same executable software module as the first executable software module.

13. The computer system of claim 10 wherein the executable software module causes the generation of access control information that indicates that the user is permitted to access a business object when (1) the user characteristic corresponds to the shared characteristic and the (2) the data object characteristic corresponds to the shared characteristic.

14. The computer system of claim 10 wherein the executable software module causes an association between at least one entry in the user information and at least one entry in the access control information when the user characteristic corresponds to the shared characteristic.

15. The computer system of claim 14 wherein the executable software module causes an association between at least one entry in the data object information and at least one entry in the access control information when the data object characteristic corresponds to the shared characteristic.

16. The computer system of claim 15 wherein the executable software module causes a determination whether the user is permitted access to the data object based on the association of the user information to the shared characteristic and the association between the data object information and the shared characteristic.

17. The computer system of claim 10 wherein:

the data repository includes:

user group information that associates a user group with at least one entry in the user information, and

access control rule information that identifies action that a user who is associated with group of users is permitted to perform on a data object, and

the executable software module causes a determination to be made, based on an association of the at least one entry in the user information with the user group, as to whether the user associated with the at least one entry in the user information is permitted to perform a particular action on a particular data object.

18. A computer-readable medium or propagated signal having embodied thereon a computer program configured to generate access control information, the medium or signal comprising one or more code segments configured to:

identify at least one entry in user information that is associated with the identified characteristic;

identify at least one entry in data object information that is associated with the identified characteristic; and

generate access control information that permits a user associated with the at least one entry in the user information to access the at least one entry in the data object information.

19. The medium or signal of claim 18 wherein the one or more code segments configured to generate access control information comprise one or more code segments configured to:

generate user access control information that identifies the at least one entry in the user information that is associated with the identified characteristic,

generate object access control information that identifies the at least one entry in the data object information that is associated with the identified characteristic, and

associate at least one entry in the user access control information with at least one entry in the data object access control information.

20. The medium or signal of claim 19 wherein the one or more code segments are further configured to determine whether a particular user associated with the at least one entry in the user access control information is permitted access to a particular data object that is associated with the at least one entry in the data object access control information wherein the determination is based on the association of the at least one entry in the user access control information with the at least one entry in the data object access control information.

21. The medium or signal of claim 18 wherein the one or more code segments are further configured to:

receive a filter condition, and

generate access control information by eliminating at least one entry in the user information that corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the user information.

22. The medium or signal of claim 18 wherein the one or more code segments are further configured to:

receive a filter condition, and

generate access control information further comprises generating access control information by eliminating at least one entry in the data object information that corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the data object information.